FOLLOW THE MONEY: U.S. ANTI-TERRORISM LAWS ON CAMPUS

ECONOMIC SANCTIONS AND ANTI- MONEY LAUNDERING/USA PATRIOT ACT ISSUES

June 25-28, 2006

M. Beth Peters, Esq.
Aleksandar Dukić, Esq.
Hogan & Hartson LLP[*]
Washington, DC

I. INTRODUCTION

You may be thinking: "*We are an institution of higher education—we don't sell widgets around the world and we don't see people on campus with paper bags full of drug money in crumpled, small-denominated bills. Do we even need to be concerned with any restrictions that the U.S. Government imposes on dealings with sanctioned countries or any provisions that are designed to prevent money laundering*?" The short answer is: Yes. U.S. economic sanctions programs impose a much wider range of prohibitions than a simple ban on exports of goods to far away rogue nations. These restrictions apply broadly to the provision of services and other types of activities such as receipt of donations or other funds, and they often target individuals who are outside the sanctioned country—in fact, they even target some persons and entities within the United States. In addition, U.S. laws designed to prevent or detect laundering of money go well beyond concerns that a bag of "dirty" money may be used to buy goods or services—they address various stages of money laundering and impose a variety of compliance and reporting obligations that are not limited to banks or other traditional financial institutions.

Education is a global, cross-border activity. Technological developments such as the Internet and easy access to web-based materials, distant learning courses, online account access, and the increased movement of people and funds across borders, require universities to establish procedures to comply with international trade control regulations. If your institution offers stored value cards, has a credit union, accepts donations or tuition payments in cash or monetary instruments such as money orders or bank drafts, or makes loans to individuals, you need to be aware of U.S. anti-money laundering restrictions designed to prevent laundering of illicit funds. This paper analyzes U.S. economic sanctions and anti-money laundering provisions including compliance and reporting obligations that apply to colleges, universities and other institutions of higher education (collectively referred to as "universities").

II. ECONOMIC SANCTIONS

A. Background

Governments around the world, as well as the United Nations, have imposed multilateral economic sanctions and trade embargoes against countries, entities, and individuals as a means to advance foreign policy and national security interests. However, the U.S. Government also imposes unilateral economic sanctions and trade embargoes which have the purpose of preventing the targeted countries, entities and individuals from benefiting from U.S. capital, goods, technology or services. This

[*] M. Beth Peters is a partner and Aleksandar Dukić is an associate with the law firm of Hogan & Hartson LLP.

creates situations where U.S. persons must comply with restrictions not imposed on our trading partners or peer institutions overseas.

B. U.S. Economic Sanctions Programs

The United States maintains comprehensive economic sanctions programs as well as more limited sanctions regimes. The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") administers and enforces both types of sanctions programs. 1/ The sanctions laws and regulations proscribe certain transactions with specific countries, entities and individuals. 2/ Penalties for violating economic sanctions laws may be civil or criminal, including monetary fines and imprisonment, and may be imposed on individuals, as well as organizations. 3/ Violations also can result in adverse publicity and reputational harm, even if the party involved were to negotiate a settlement with OFAC.

1. Sanctioned Countries

The U.S. Government currently maintains comprehensive economic sanctions against four countries: ***Cuba***, ***Iran***, ***Sudan*** and ***Syria***. 4/ More limited economic sanctions are currently in effect against: ***Burma (Myanmar)***, ***Iraq***, ***Liberia*** and ***North Korea***. In addition, the U.S. Government has imposed economic sanctions against certain senior members of the Government of Zimbabwe and certain entities owned or controlled by them as well as against certain persons who are contributing to the conflict in the Ivory Coast (Côte D'Ivoire). These sanctions are not territorial in nature (i.e., they do not apply to Zimbabwe or the Ivory Coast as a whole or to their governments as a whole), and they only target designated persons and entities in their individual capacity.

2. Specially Designated Nationals (SDNs)

The U.S. sanctions programs also prohibit transactions with persons and entities designated as terrorists, sponsors of terrorist activity and terrorist organizations, narcotics traffickers and kingpins, agents of sanctioned country governments, and proliferators of weapons of mass destruction. These persons and entities are designated by the U.S. Government as Specially Designated Nationals or Blocked Persons (SDNs) and are included on the SDN list, which is maintained by OFAC. 5/ The SDN list currently contains more than 6,000 entries, including the names of individuals and entities, as well as other known information (e.g., aliases, date of birth, last known residential or business address, passport

---

1/ More information about OFAC and U.S. sanctions programs is available at http://www.treas.gov/offices/enforcement/ofac/index.shtml.

2/ OFAC regulations governing U.S. economic sanctions programs are found at 31 C.F.R. Parts 500-598.

3/ For most sanctions programs, civil penalties now include a fine of up to $50,000 per violation (for the Cuban sanctions, the fine is up to $65,000 per violation; for violations of the Narcotics Kingpin Act sanctions, the fine is up to $1.075 million). Until recently, the civil penalty amount was limited to $11,000 per violation. The USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177 (H.R. 3199), which was signed into law on March 9, 2006, amended the International Emergency Economic Powers Act (IEEPA) by increasing the maximum amount of a civil penalty from $11,000 to $50,000. Also, the criminal penalty for willful violations by individuals has been increased from 10 to 20 years imprisonment.

4/ U.S. sanctions against Libya were lifted on September 20, 2004, and all property previously blocked pursuant to the sanctions has been unblocked. However, Libya remains on the list of terrorist supporting countries and, as a result, remains subject to tighter export controls.

5/ The SDN list is available at http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf.

number etc.). OFAC regularly updates the SDN list due to frequent additions of newly designated persons and entities (occasionally, certain entries are removed from the SDN list).

3. Scope of Restrictions

Under the comprehensive U.S. sanctions programs, a "U.S. person" generally may not, without a license or authorization from the U.S. Government, 6/ engage in any of the following:

- Export or import, directly or indirectly, goods, services or technology to and from, a sanctioned country;
- Enter into a contract involving, or otherwise provide services to, a sanctioned country, including an entity or individual located in a sanctioned country;
- Engage in any transaction with persons and entities designated as SDNs;
- Approve or facilitate any of the above activities; and
- Evade provisions of the sanctions regulations.

U.S. persons also must "block" (freeze) property and property interests of SDNs, and certain sanctioned country governments, that are within the possession or control of a U.S. person. 7/ This includes funds received from or held on behalf of, or a contract involving, an SDN. For example, a U.S. person who receives a payment from an SDN must place such funds into a blocked, interest-bearing account at a U.S. financial institution. In addition, the receipt of such blocked property must be reported to OFAC, as set forth in Section II.C below. Similarly, if a U.S. person has an existing contract with a person who subsequently becomes an SDN, the U.S. person must "block" such contract on its books, preventing any further activity or performance under the contract, and must file a blocked property report with OFAC.

The prohibitions on exportation and importation of services generally are very broad and apply to services provided or received, directly or indirectly, to or from a sanctioned country or an SDN (e.g., maintaining an account in the United States for a person residing in Iran generally is considered a prohibited exportation of a financial service to Iran). In addition, the comprehensive U.S. sanctions programs have broad prohibitions on approval and facilitation by U.S. persons. 8/ For example, U.S. persons are prohibited from participating in, approving or facilitating, aiding or otherwise supporting activities by foreign persons involving a sanctioned country where such actions would constitute violations of the sanctions if engaged in by a U.S. person. Similarly, OFAC interprets the facilitation provision to prohibit a U.S. person from altering its operating policies or procedures, or those of a foreign affiliate, in order to permit a foreign affiliate to engage in transactions involving a sanctioned country that previously required the approval or participation of the U.S. person. Moreover, OFAC

6/ There are comprehensive OFAC sanctions against Cuba, Iran, and Sudan; while the OFAC sanctions against Syria currently are narrow, the U.S. export controls are extremely broad. For most sanctions programs, authorization to conduct a transaction is obtained from OFAC; for certain transactions, U.S. persons must file requests for authorization with the Commerce Department's Bureau of Industry and Security (BIS).

7/ Not all of the country-specific sanctions programs have "blocking" provisions (for example, the current U.S. sanctions against Iran do not block the property of the Government of Iran). The broadest restrictions are in the Cuba sanctions program. The terms property and property interests are defined broadly to include all forms of financial interests, whether tangible or intangible, such as bank deposits, savings accounts, real property, leases, letters of credit, money, securities, as well as contracts of any nature. *See generally* 31 C.F.R. §§ 515.311, 538.310.

8/ *See generally* §§ 538.206, 538.407, 560.208, 560.417.

regulations prohibit U.S. persons from engaging in any transaction that evades or avoids, or has the purpose of evading or avoiding, the restrictions imposed by U.S. sanctions programs.

All of the U.S. sanctions programs apply to "U.S. persons," which is defined broadly to include:

- Entities organized under U.S. law, and their employees (e.g., U.S. corporations, U.S. institutions and organizations);
- All U.S. citizens and U.S. lawful permanent residents (also known as "green card" holders) wherever they are located;
- All people and organizations physically present in the United States, regardless of citizenship; and
- All foreign branches of U.S. businesses and other U.S. organizations.

For purposes of U.S. sanctions against Cuba and North Korea, however, the sanctions apply more broadly to "persons subject to U.S. jurisdiction," which is defined to include foreign-incorporated subsidiaries of U.S. companies as well. 9/

4. Sanctions Exposure for Universities

Although U.S. universities primarily engage in activities within the United States, increasingly there are areas of potential sanctions exposure and numerous ways for universities to encounter sanctions issues. Specifically, universities could face sanctions exposure when:

- Accepting tuition payments from, or making grant payments to, a student who is or becomes an SDN;
- Accepting donations from an SDN;
- Providing services online (e.g., through a distance learning program) to students in certain sanctioned countries (e.g., Cuba, Iran, Sudan);
- Hiring an employee, or entering into an agreement with a vendor, who is or becomes an SDN;
- Dealing with foreign students and professors from sanctioned countries who wish to engage in research restricted by U.S. export controls;
- Sending employees, students or alumni on a trip to a sanctioned country;
- Hiring persons in sanctioned countries to perform services for the university or its professors such as research or field work;
- Making certifications in grant applications or other contracts regarding university compliance with sanctions laws;
- Collaborating on research projects with persons or entities from certain sanctioned countries (even if the persons are not SDNs); and
- Maintaining credit union accounts for students from sanctioned countries who have returned home after completing their studies in the United States.

The vast majority of SDNs are located outside the United States, which reduces the risk of exposure for U.S. universities with respect to enrolling students and hiring employees in the United States as well as with respect to entering into vendor agreements and other contracts with U.S.

9/ *See id.* §§ 500.329, 500.330. This definition also includes any entity owned or controlled by "U.S. persons."

companies. That said, universities should not merely rely on geography or U.S. citizenship status as a method to address sanctions compliance because some SDNs are located in the United States, 10/ while others have U.S. social security numbers 11/ or were born in the United States. 12/

Moreover, all citizens of Cuba (except those who are in the United States) and all entities owned or controlled by the Cuban Government or citizens of Cuba are considered SDNs, even though they are not specifically named on the SDN list. As a result, the universities should consider the appropriate compliance activities to address the aforementioned risk exposure (see Section II.B.7 below for more details regarding sanctions compliance and screening activities).

Case Study: A professor is working on a research project and needs empirical data regarding the growth rate of a rare plant in Sudan. He knows a research institute in Sudan and wants to hire their researcher to observe the plant and record the results.

Q. Can the professor do this, with or without the university's assistance?

A. No, neither the professor nor the university could hire a person in Sudan without a specific license. OFAC regulations prohibit the importation of services from Sudan. By hiring a person in Sudan to perform the work, the professor (or the university) would be importing his/her services, which is prohibited under U.S. law, even if that person is not an SDN of Sudan. The university could apply for a license from OFAC to authorize the activities.

Q. Can the professor travel himself to Sudan and watch the plant grow?

A. Yes. Travel to Sudan is not prohibited (see Section II.B.6 below for more information related to travel activities). However, if the professor needs to take his/her laptop or technical information related to the research or engage in other activities in Sudan, the professor (and/or the university) needs to analyze sanctions and export control law provisions to determine whether such export is permitted (e.g., whether the laptop contains encryption software etc.). If the university is reimbursing any of the expenses for these activities, or authorizing the travel, the university should independently review the nature of the proposed activities.

5. Exceptions Applicable to Universities

Universities generally may enroll students or hire staff who are citizens of Cuba, Iran or Sudan if they are U.S. permanent residents ("green card" holders) or if they are lawfully present in the United States pursuant to a valid visa (*e.g.*, F, J, H, M, O, etc.). The current sanctions programs against Burma, Iraq, Liberia, North Korea and Syria do not prohibit the exportation or importation of educational

10/ For example, Richard A. Chichakli in Texas, AERO Continente Inc. in Florida, Al-Haramain (U.S. branch) in Oregon, Ash Trading Inc. in Florida, Holy Land Foundation in Texas, IAC International Inc. in Florida, and Sepulveda-Iragorri Inc. in Florida.

11/ For example, Julio C. Flores Monroy, Gregorio Gonzales Lopez, Raed M. Hijazi, and Abu Ahmad.

12/ For example, Abdul Rahman Taha.

services (but the sanctions against Burma do prohibit the exportation of financial services to Burma, which includes payments to Burma). Therefore, universities may enroll students or hire staff who are citizens of Burma, Iraq, Liberia, North Korea and Syria, provided that the individuals are not SDNs.

Even if students are enrolled, the university should be sensitive to certain issues that may still arise. For example, if foreign students from a sanctioned country such as Iran or Sudan were to return to their home countries after completing their stay in the United States in F-1 foreign student or similar nonimmigrant visa status, universities should no longer maintain credit union or other accounts on their behalf because such activities likely would be viewed by OFAC as a prohibited exportation of services to a person in Iran or Sudan. As noted above, while the term "services" is not defined in the regulations, OFAC interprets the term broadly.

U.S. export control laws restrict the ability of universities to grant access to foreign nationals present in the United States to certain types of technology and technical data controlled under the International Traffic in Arms Regulations (ITAR), which are administered by the State Department's Directorate of Defense Trade Controls (DDTC), or those controlled under the Export Administration Regulations (EAR), which are administered by the Commerce Department's Bureau of Industry and Security (BIS). 13/ Universities may be able to rely on certain exemptions under the export control laws, including those related to "publicly available" information. For example, the "fundamental research" exemption allows foreign national students to participate in research activities involving controlled technologies if the results of the research would be published. 14/

OFAC regulations generally do not prohibit universities from providing "information" and "informational materials" to persons in sanctioned countries. Under the applicable regulations, information and informational materials generally include but are not limited to publications, films, posters, photographs, microfilms, compact disks, CD ROMs, and certain artworks. However, only information and informational materials that have been fully created and in existence at the date of the transaction can qualify for this exemption. 15/ Please note that the substantive or artistic alternations or enhancement of informational materials and the provisions of marketing or business consulting services do not qualify for this exemption. This exemption enables universities to provide online access to persons in a sanctioned country to certain information related to the university. Specifically, universities are not prohibited from allowing persons in sanctioned countries from reviewing information posted on the university website, such as general information about the institution, course selection, course schedule and similar information. If, however, the university's website were to offer an operational component that allows users to conduct real-time transactions based upon their review of the information transmitted (e.g., registering for courses, taking online tests, making tuition payments, initiating funds transfers or payments from credit union accounts etc.), those transactions would be

---

13/ For more information about the scope of the ITAR and EAR and the relevant "deemed export" and immigration issues involving foreign nationals physically present in the United States, please see the following articles by M. Beth Peters et al. *"Foreign Nationals in U.S. Technology Programs: Complying With Immigration, Export Control, Industrial Security and Other Requirements,"* Immigration Briefings No. 00-10 (Oct. 2000); *"Complying With Immigration, Export Control, and Industrial Security Requirements When Working Collaboratively With Foreign Nationals: A Case Study,"* The International Lawyer, Vol. 35, No. 1 (Spring 2001).

14/ *See* 15 C.F.R. §§ 734.3(b)(3), 734.8; 22 C.F.R. §§ 120.10(5), 120.11(8). *See also* supra note 13.

15/ Please note that the informational materials exemption under OFAC regulations does not pertain to exportation of information, including software and technical data, subject to licensing requirements under the EAR, ITAR, or governed by the Department of Energy or other government agencies.

beyond the scope of the exemption and would viewed by OFAC as prohibited exportation of services if a person in a sanctioned country were to conduct them online via the university's website. 16/

With respect to the peer review process, which was previously analyzed by OFAC under the "informational materials" exemption and was subject to a more restrictive interpretation, 17/ OFAC issued new general licenses in December 2004 to authorize certain activities by U.S. persons that directly support the publishing of manuscripts, books, journals and newspapers and that were not previously covered by the "informational materials" exemption. 18/ Pursuant to these general licenses, U.S. reviewers can engage in certain activities related to the publishing of articles that were authored by persons in Cuba, Iran and Sudan. For example, the authorized activities include: collaborating on the creation and enhancement of written publications; augmenting written publications through the addition of items such as photographs, artwork, translation and explanatory text; substantive editing of written publications; and, other transactions necessary and ordinarily incident to the publishing and marketing of written publications. However, these general licenses also contain important exclusions, specifying that U.S. persons cannot: (1) engage the services of a publishing house or a translator in one of these sanctioned countries (unless such activity is primarily for the dissemination of written publications within the sanctioned country); (2) engage in transactions involving the provision of goods or services not necessary and ordinarily incident to the publishing and marketing of written publications (e.g., cannot provide or receive individualized or customized services such as accounting, legal, design or consulting services); (3) engage in transactions for the development, production, design, or marketing of software; (4) engage in transactions that involve the government of the sanctioned country, or its agencies or instrumentalities (for the purposes of these licenses, the term "government" does not include any academic or research institutions and their personnel); and (5) engage in transactions involving ITAR-controlled technology or export information controlled under the ITAR or the EAR. 19/

Because exemptions and general licenses under OFAC regulations generally are complex and the analysis is fact-specific, professors and university staff should seek legal advice before making a final determination whether the export of a particular item or the provision of a particular service is covered by a general license or exempt from OFAC and BIS restrictions.

6. Travel

Most sanctions programs do not restrict the ability of U.S. persons to travel to a sanctioned country, with the exception of the U.S. sanctions against Cuba. While travel itself may not be restricted, the activities which are to be pursued within a sanctioned country or the items or technical data to be brought into the country may be restricted, depending on the destination. U.S. sanctions also restrict the ability of U.S. persons to import certain items into the United States after their travel to a sanctioned

---

16/ In its prior rulings that dealt with a Computerized Reservation System ("CRS"), which allows real-time access to schedule, pricing and availability information for airlines, lodging and rental car companies, OFAC held that review and sharing of such information qualified for the "information and informational materials" exemption but that no operational transactions could be conducted through the CRS based on the customer's review of the information transmitted. *See* OFAC Ruling 020416-FACRL-CU-01 (Apr. 16, 2002) at www.ustreas.gov/offices/enforcement/ofac/programs/common/ltr041602.pdf (addressing restrictions under the Cuban Assets Control Regulations and citing a prior OFAC ruling from January 1995 that also dealt with a CRS).

17/ *See* OFAC Ruling 040405-FARCL-IA-15 (Apr. 2, 2004) at www.ustreas.gov/offices/enforcement/ofac/programs/common/ia040504.pdf.

18/ *See* 31 C.F.R. §§ 515.577 (Cuba), 538.529 (Sudan), 560.538 (Iran).

19/ *Id.*

country. For example, U.S. persons may not be able to take along certain laptops, testing equipment, or technical data to a sanctioned country such as Iran, Sudan or Syria, even though they are not prohibited from traveling there. Accordingly, prior to traveling to a sanctioned country, the contemplated activities and the items needed for the trip should be reviewed and assessed in order to ensure compliance with OFAC regulations and/or U.S. export control laws and regulations.

The Cuban Assets Control Regulations (CACR) 20/ prohibit U.S. persons from traveling to Cuba without a license. Travel to Cuba may be authorized pursuant to a general license set forth in the CACR or a specific license, which would be approved on a case-by-case basis by OFAC. 21/ Licenses may be granted for a variety of types of activities, including journalistic activity, professional research, educational activities, religious activities, public performances, and activities of private foundations or research or educational institutes. For example, OFAC's general license authorizes full-time professionals to travel to Cuba to conduct professional research. 22/ In order to qualify under this general license, the research would have to be noncommercial and academic in nature, comprise a full work schedule in Cuba, and have a "substantial likelihood" of public dissemination. 23/ OFAC's general license also authorizes full-time professionals to travel to Cuba to attend professional meetings or conferences organized by an international professional organization, institution, or association that regularly sponsors meetings or conferences in other countries. 24/ In order to qualify for this general license, the purpose of the meeting must not be the promotion of tourism or other commercial activities in Cuba and the meeting must not be intended primarily for the purpose of fostering production of any biotechnological products. 25/ In general, specific terms of the CACR should be reviewed carefully to ensure that the contemplated activities in Cuba meet the conditions and requirements of OFAC's general or specific licenses for travel to Cuba.

In addition to assessing a possible basis for licensed travel under the CACR (i.e., whether a general license applies or whether a license application should be submitted to OFAC seeking specific authorization for the contemplated activities), universities and intending travelers also should review OFAC's "Comprehensive Guidelines for License Applications to Engage in Travel-Related Transactions Involving Cuba," which contain information about general and specific licenses, including the license application process. 26/ Individuals planning to travel to Cuba should be mindful of restrictions on the maximum daily spending allowance, which is currently set at $177, including meals and lodging. 27/ There are also restrictions on what individuals returning from Cuba may bring back to the United States (e.g., U.S. persons may no longer bring back Cuban cigars for personal consumption).

20/ 31 C.F.R. Part 515.

21/ *See id.* §§ 515.560 *et seq.*

22/ *Id.* § 515.564(a)(1).

23/ *Id.* Note, however, that activities set forth in paragraphs (c), (d), and (e) of section 515.564 would not qualify for this general license (e.g., research for personal satisfaction or travel in pursuit of a hobby would not qualify for this general license authorizing travel for professional research).

24/ *Id.* § 515.564(a)(2).

25/ *Id.* Note that the general license requires that the meeting organizer be headquartered outside the United States, unless the organizer is a U.S. institution or organization that was specifically licensed by OFAC to sponsor the meeting in Cuba.

26/ The guidelines are available at: http://www.treas.gov/offices/enforcement/ofac/programs/cuba/cuba_tr_app.pdf.

27/ Before going to Cuba on a licensed trip, travelers should check for updated per diem rates at: http://www.state.gov/m/a/als/prdm/.

Case Study: One of our university professors wants to take his class on a two week trip to Cuba to visit a Cuban university, observe their classes and participate in discussions with Cuban counterparts. The professor and his students would attend classes in the mornings and would spend afternoons exploring Cuban's cultural heritage.

Q. Can the university get a travel license for its professor and students?

A. Not likely. A specific license could be obtained for educational activities but it would require participation in a structured educational program in Cuba for no less than 10 weeks. 28/ Also, the contemplated activities would fall outside the scope of general licenses for professional research activities and professional meetings in Cuba. Even if the class were to stay in Cuba for 10 weeks as part of a structured program, all travelers need to be mindful of restrictions on expenditures in Cuba (per diem) and the restrictions on importation of Cuban-origin goods back to the United States.

7. Compliance and Screening

OFAC regulations do not mandate that U.S. universities or companies use screening software to check persons or entities against the SDN list in order to ensure compliance with U.S. sanctions programs. Because the applicable regulations prohibit any dealings by U.S. persons with individuals or entities on the SDN list, the use of screening software is advisable, especially when there is a large number of persons or transactions that need to be screened. Of course, a university could achieve compliance by manually comparing the names to the entries on the SDN list, which is available online as described above, but this approach may not be feasible if the university is trying to screen a large number of names or transactions (e.g., all applicants for admission or all deposits and wire transfers into credit union accounts).

The best way to ensure compliance is by:

- Determining whether a person or entity from a sanctioned country is involved in the contemplated transaction; and
- Checking the names of the persons involved against the SDN list (either manually, using the list published on OFAC's website, or through the use of a screening software).

Because the SDN list changes frequently, as newly designated persons or entities are added, regular vigilance is necessary. To ensure compliance, screening should be done on a regular basis. If the university were to conduct screening only at the outset of a relationship, it would ensure that the university can engage in the contemplated transaction (e.g., enroll a student, hire an employee, or enter into a vendor contract) but that approach would not capture any subsequent changes that may affect the relationship. Without periodic screening, there would be some exposure for the university because it would be unaware if students, staff members, vendors or other contract parties subsequently became designated as SDNs or if they were subject to new sanctions programs. As such, the university would not be able to comply timely with the blocking and reporting obligations and could inadvertently be conducting transactions that it is no longer authorized to perform (e.g., while it is permitted to make loan disbursements to a student before his/her SDN designation, no payments could be made to him/her after

28/ *See* 31 C.F.R. § 515.565 (setting forth the requirements for attendance of a program in Cuba and activities related thereto for which a specific license from OFAC may be requested).

the designation, absent a specific license from OFAC). In light of the volume of university records and frequency of changes on the SDN list, the easiest way to ensure compliance is through periodic, automated screening. The interval in which an entity conducts "batch" screening is based on the entity's assessment of its OFAC-related risks.

Case Study: A student from Colombia is currently in his sophomore year at the university and has an account with the university's credit union. The student's father, who is still living in Colombia, periodically wires funds to the student's account at the credit union, which the student uses to pay tuition and other university charges for each semester. On January 5, 2006, OFAC designated the student's father as an SDN, due to his involvement as part of the Cali Cartel. On January 7, 2006, the university credit union received a funds transfer from the father in the amount of $25,000 for the student's spring semester expenses. The credit union deposited the funds in the student's account. On January 20, 2006, a university employee reads in the newspaper that OFAC designated a number of narcotics traffickers from Colombia as SDNs and recognizes the name of the student's father who is also mentioned in the article.

Q. Can the credit union return the money to the father because it does not want to have any dealings with a narcotics trafficker?

A. No. The credit union cannot refuse to accept the funds transfer in this case and it cannot return the money to an SDN. Instead, the credit union is now in possession of SDN's property or property interest ($25,000) and such funds must be placed in a blocked, interest-bearing account at the credit union or at another U.S. financial institution. The funds cannot be disbursed to the student and he cannot be allowed to withdraw or otherwise dispose of those funds. The student could continue to attend classes because he has not been designated as an SDN; however, he will not be able to use the funds sent, directly or indirectly, by his father because those funds must be blocked by U.S. persons.

In addition, the university's credit union was required to file a blocked property report with OFAC by January 17, within 10 days of the receipt of the SDN's funds (see Section II.C below for more details). Because the designation was discovered by chance on January 20, the credit union is already late with respect to its reporting obligation. By not having a screening mechanism that runs nightly or weekly batch screening of deposits and incoming wire transfers, the credit union was unable to timely block the funds and prevent their withdrawal; also, the credit union was unable to prepare and file a timely blocked property report.

C. Reporting Requirements

Under OFAC regulations, U.S. persons are required to file a blocked property report with OFAC within 10 days of receiving funds from an SDN (or within 10 days from the date a person or entity is designated as SDN if, at the time of the designation, the U.S. person has an existing contract with, or holds funds in an account on behalf of, the person or entity designated as SDN). In addition, blocked property reports must be filed if the U.S. person receives funds from, or holds funds on behalf of, a sanctioned country government (or any of its agencies, instrumentalities, or entities owned or controlled by it) that is subject to the blocking provisions, such as Cuba and Sudan. After filing the initial blocked

property report, a U.S. person must also file an annual report, listing all blocked property received over the course of the year.

III. ANTI-MONEY LAUNDERING/USA PATRIOT ACT

A. Background

The United States imposes anti-money laundering (AML) restrictions to protect the integrity of the U.S. financial sector and to prevent criminals and terrorists from abusing the U.S. financial system for their illicit activities. Money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them. Through money laundering, the criminal transforms the monetary proceeds derived from criminal activity into funds with an apparently legal source. There are three stages to money laundering:

1. *Placement* – illegally derived funds are placed into the stream of commerce;
2. *Layering* – one or more transactions to disguise the true source of the funds; and
3. *Integration* – money is repatriated into the economy in its disguised form, with the appearance of being "clean" and coming from a legitimate source. 29/

Most people think of the placement stage as "the" money laundering. However, the other two stages also are an integral part of the process and those two stages may involve transactions with businesses and institutions, such as universities, that are not typically viewed as "gatekeepers" for AML purposes. In order to track the flow of funds, the U.S. Government has established a fairly complex reporting system, through the Bank Secrecy Act, 30/ as amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), 31/ Treasury regulations, and the Internal Revenue Code ("IRC"). As explained below, certain reporting obligations apply to all businesses and institutions in the United States. The BSA also contains additional AML provisions that apply to a wide range of "financial institutions," which are very broadly defined to include businesses and institutions beyond those traditionally viewed as financial.

Because terrorists engage in money laundering to fund their illicit activities, U.S. AML laws and regulations also are designed to disrupt and prevent terrorism-related money laundering activities. Furthermore, the same laws strive to disrupt and prevent terrorist financing, which represents the

---

29/ For example, a person deposits $50,000 of "dirty" money at a U.S. or a foreign bank account (*Placement*), through a series of small cash payments in an attempt to avoid triggering the reporting threshold (the practice known as "structuring" or "smurfing"). The person then sends those $50,000 by wire transfer to a U.S. account in a student's name, or to another person's account who then transfers to the student's bank account (*Layering*). Finally, the student uses that money to pay for tuition, room and board, overpaying the charges by $17,000; the student then seeks reimbursement of the overpayment and receives a check for $17,000 from the university (or receives a stored value card with the same amount), representing "clean" money (*Integration*).

30/ 31 U.S.C. § 5311 *et seq.*

31/ Pub. L. 107-56 (Oct. 26, 2001). Title III of the USA PATRIOT Act, which is titled the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, provides the Secretary of the Treasury and other departments and agencies of the federal government with enhanced authority to identify, deter, and punish international money laundering.

opposite of money laundering (i.e., legally derived funds are used for illicit activities, to fund terrorist acts or organizations).

U.S. laws designed to prevent and detect money laundering and terrorist financing are administered by the Treasury Department's Financial Crimes Enforcement Network (FinCEN).32/

B. AML Provisions in the Bank Secrecy Act/USA PATRIOT Act

As described in more detail below, there are certain AML provisions under U.S. law that apply to all businesses and institutions in the United States, such as the obligation to report the receipt of cash in excess of a certain amount or the receipt of cash that was physically transported across U.S. borders (also in excess of a certain amount). These provisions predate the enactment of the USA PATRIOT Act and all universities should be aware of, and must comply with, these reporting obligations. The majority of AML provisions addressed in this section, however, apply only to covered "financial institutions," as that term is broadly defined under the BSA.

1. The Definition of "Financial Institution"—Are Universities Covered?

The term "financial institution" is broadly defined in the BSA to include businesses beyond those traditionally viewed as financial institutions such as banks and credit unions—specifically, the definition also includes money services businesses (MSBs, which include but are not limited to issuers, sellers or redeemers of "stored value"), "loan or finance companies," casinos, pawnbrokers, dealers in jewels and precious metals, car dealers, persons engaged in real estate settlements and closings, etc. 33/ Because universities may have credit unions, issue stored value cards, and make loans to students, a closer examination may be required in order to determine whether a particular university, or its part, could be viewed as "financial institutions" under the BSA and thus become subject to its AML provisions.

University credit unions clearly are covered "financial institutions" and must comply with the applicable BSA requirements. The entire university, however, would not become subject to the BSA simply by having a credit union; instead, the credit union itself must comply with various AML provisions and the university might be exempt, unless it engages in other activities that may be covered by the BSA.

Universities that issue stored value cards should assess whether they are covered by the BSA as MSBs. The MSBs includes issuers, sellers or redeemers of "stored value." 34/ The BSA regulations expressly exclude from the MSB definition those entities that who only issue, sell or redeem "stored value" in an amount of $1,000 or less to any person on a single day in one or more transactions (e.g., hotels that limit the issuance of their stored value cards to $600 per day and do not issue more than one card to a single individual, would be exempt from the definition of MSBs). 35/ Assuming that the university issues to its students stored value cards (SVCs) with a semester's worth of meal plan money, the $1,000 threshold likely would be exceeded in a single transaction and this exemption would not apply. Consequently, the university has to analyze the nature of its SVC practices as a basis for a possible exception from the regulatory requirements.

32/ More information about FinCEN is available at: http://www.fincen.gov/index.html.
33/ *See* 31 U.S.C.A. § 5312(a)(2).
34/ *See* 31 C.F.R. § 103.11(uu)(3)-(4).
35/ *Id.*

FinCEN has issued a ruling that is applicable to situations where the university only issues "closed" system SVCs (e.g, cards that can only be used to pay for university-related goods and services, and possibly to pay for goods and services of designated merchants or vendors on campus, or in its vicinity). 36/ While the final rule implementing BSA provisions for MSBs does not explicitly exclude closed system SVCs from the definition of "stored value," the preamble to the final rule leaves room for further rulemaking on "specific issues such as, for example, exemptions for 'closed system' or small denomination stored value devices." 37/ Further, in an August 2003 ruling, FinCEN states that the definition of "stored value" is not currently interpreted by FinCEN to include "closed system products such as a mall-wide gift card." 38/ Based on this ruling, universities with "closed" system SVCs would have an argument that they are not MSBs within the meaning of the BSA. In addition, the U.S. Government recently acknowledged that closed system SVCs present "more limited opportunities and a correspondingly lower risk" of money laundering. 39/ Because federal law enforcement agencies have seen both categories of SVCs (open and closed system) being used as "alternatives to smuggling physical cash," 40/ FinCEN continues to monitor these law enforcement concerns.

The Treasury Department is taking a risk-based, industry-specific approach in issuing regulations to implement various BSA/USA PATRIOT Act provisions. As a result, it has yet to issue rules applicable to "loan or finance" companies and define the scope of that term (also, FinCEN has yet to issue rules for a host of other types of non-traditional financial institutions such as car dealers, persons engaged in real estate closings and settlements, etc.). Accordingly, it is not presently clear whether universities, due to their student loan activities, would be considered "loan or finance companies" and thus covered as a financial institution under the BSA. Universities should review their activities and continue to monitor FinCEN's rulemaking and regulatory developments. After FinCEN issues a proposed rule for "loan or finance companies," universities will need to determine whether they are covered by the definition of that term.

Based on the foregoing, universities with no credit unions and with only "closed system" SVCs currently are not subject to specific AML provisions in the BSA that apply to "financial institutions" (as a result, such universities only are subject to reporting requirements that apply to all U.S. businesses and institutions, as set forth in Sections III.C.2 and C.3 below). University credit unions are required to comply with all of the AML provisions described below.

2. Key AML Provisions That Apply to "Financial Institutions"

Key AML provisions in the BSA, as amended by the USA PATRIOT Act, that currently apply to "financial institutions" such as credit unions are:

- **Sec. 352** – AML Compliance Program Requirements

36/ "Open" system SVCs, as opposed to closed system cards, can be used to connect to global debit and ATM networks, allowing purchases at any merchant or access to cash at any ATM that connects to the same network (e.g., Visa's or MasterCard's global networks).

37/ 64 Fed. Reg. 45438, 45442 (Aug. 20, 1999).

38/ FinCEN Ruling 2003-4 (Aug. 15, 2003), *available at* www.fincen.gov/fincenruling2003-4.pdf.

39/ "U.S. Money Laundering Threat Assessment" (Dec. 2005), p. 20, *available at* www.ustreas.gov/offices/enforcement/pdf/mlta.pdf.

40/ *Id.* at p. 21.

- **Sec. 326** – Customer Identification and Verification Requirements (also known as "Know Your Customer" or "KYC" requirements)
- **Sec. 314(a)** – Information Sharing and Cooperation with Law Enforcement
- **Sec. 311** – Designation of "Primary Money Laundering Concerns" and Imposition of "Special Measures" against such designated entities or jurisdictions.

3. Section 352 – AML Compliance Programs

Section 352 requires covered financial institutions such as credit unions to establish and implement an AML Compliance Program, based on a "risk assessment" of its products and services (accordingly, lower risk products/services or transactions may warrant fewer procedural controls). Each AML program must contain the following: (1) designation of a compliance officer; (2) establishment of internal policies, procedures, and controls; (3) provision for employee training; and (4) an independent audit function. As appropriate, a credit union may delegate a part of the required AML functions to other persons (i.e., agents) but liability for their actions is retained by the credit union, with limited exceptions.

The institution's AML Compliance Program should have support from its Board and top officers and should give the Compliance Officer sufficient authority to carry out his/her responsibilities. With respect to the independent audit function, the Program cannot provide that the Compliance Officer would also act as an "independent" auditor. The audit function does not have to be performed by someone outside the institution but it cannot be performed by the Compliance Officer or anyone within his/her compliance organization. The Program should also provide for reporting to the Board or senior officers and mandate formal employee training. The training may be conducted in-house and does not have to include all employees—the training could be limited to employees whose responsibilities involve tasks or related to duties addressed by the AML Compliance Program. Those employees need to be trained with respect to the internal policies, procedures and controls that have been implemented to address AML compliance.

Policies supporting the institution's AML efforts include:

- Conducting risk assessment of the institution's activities and services;
- Identifying high risk transactions and communicating "red flags" to relevant employees;
- Monitoring account transactions, including attempted "structuring" or "smurfing" (employees should not focus exclusively on the "placement" stage and should be mindful of possible abuse through "layering" and "integration");
- Requiring reporting of suspicious transactions and cash transactions (as set forth in Section III.C below, the institution has to determine whether reporting of a cash transaction is required (by filing the 8300 form) or whether a Suspicious Activity Report (SAR) is required or warranted in a particular case);
- Establishing "Know Your Customer" procedures, which may be integrated within the AML Compliance Program.

4. Section 326 – Customer ID/Verification ("Know Your Customer")

Section 326 requires covered financial institutions such as credit unions to establish and implement a Customer Identification Program ("CIP"), which also can be risk-based and appropriate for

the size and type of activity involved. 41/ The purpose of a CIP is to identify the institution's new customers and to verify their identity. The CIP requirements include the following:

- Obtaining identifying information from a person seeking to open a new account (the BSA regulations specify information that needs to be obtained as part of the customer identification process, such as name, address, date of birth and a taxpayer identification number for customers who are individuals); 42/
- Verifying the identity of such person, using reasonable procedures for identifying persons and entities (the BSA regulations provide guidance with respect to verification based on documents or through non-documentary means); 43/
- Developing procedures responding to circumstances where a reasonable belief about the true identity cannot be formed and where additional verification is required;
- Maintaining records of identifying information;
- Determining whether the person appears on any lists of known or suspected terrorist or terrorist organization provided by any government agency (at present, the covered financial institutions are only required to screen the customer's name against OFAC's SDN list because the U.S. Government has not yet issued a list that is specific to the CIP requirements under sec. 326).

5. Section 314 – Information Sharing

Section 314(a) imposes information sharing requirements on covered financial institutions such as credit unions. A law enforcement agency that wants to search the records of a particular financial institution to see whether a person or entity that is the target of an investigation is maintaining account(s) or other relationship(s) with U.S. financial institutions can submit a request to FinCEN. Upon reviewing the request, FinCEN would make a determination whether the request qualifies for section 314(a) purposes and, if so, FinCEN would send the request to one or more financial institutions. The request from FinCEN may ask the institution to search its records for any information on a particular person or entity identified in the request.

There is no exemption for university credit unions from section 314(a) information requests from FinCEN. FinCEN informally advised that 314(a) requests are being sent only to financial institutions that are required to have an AML program, such as banks, credit unions etc. (i.e., they are not being sent to "loan or finance companies"). Credit unions should be prepared to receive a section 314(a) request (designating one or more persons to take action on a request).

6. Section 311 – "Primary Money Laundering Concerns"

Section 311 authorizes the U.S. Government to designate entities or jurisdictions as "primary money laundering concerns" (PMLC) and to impose one or more of the "special measures" authorized by the statute. The most comprehensive special measure involves a requirement that covered U.S. financial institutions terminate all correspondent account relationships with PMLCs and to prevent existing correspondent accounts held on behalf of third parties to be used indirectly for or on the benefit of PMLCs. The PMLC determinations by the U.S. Government and related imposition of special

41/ *See* 31 C.F.R. § 103.121.
42/ *Id.* § 103.121(b)(2)(i).
43/ *Id.* § 103.121(b)(2)(ii).

measures should not affect credit unions, unless they have correspondent account relationships with foreign banks.

To date, the U.S. Government has taken the following actions pursuant to authority set forth in section 311: 44/

- **Nauru**—designated as PMLC and "special measures" were proposed (termination of correspondent accounts involving Nauru financial institutions);
- **Burma and 2 Burmese banks**—designated as PMLCs and "special measures" were imposed (termination of correspondent accounts);
- **Commercial Bank of Syria (CBS)**—CBS and its subsidiary were designated as PMLCs (Syria as a country, however, has not been designated as PMLC) and "special measures" were imposed (termination of correspondent accounts).

7. Other Provisions of Interest to Universities

Additional provisions set forth in the BSA, as amended by the USA PATRIOT Act, may be triggered if a particular credit union:

- Is maintaining correspondent or "payable through" accounts for foreign banks;
- Is offering private banking accounts to any non-US person; or
- Is maintaining or administering accounts for a "shell bank." 45/

Also, if the university uses an "open" system SVC and does not limit the issuance of such SVC to no more than $1,000 per person per day, the university would need to analyze whether it would be considered an MSB and thus subject to the BSA requirements. Specifically, MSBs are required to have an AML Compliance Programs under section 352. However, SVC issuers do not have to register with FinCEN and are not subject to mandatory SAR reporting (unlike other MSBs).

8. Financial Action Task Force (FATF)

On the international level, the Financial Action Task Force on Money Laundering (FATF) is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing (http://www1.oecd.org/fatf). FATF issues recommendations to its members and maintains a list of Non-Cooperative Countries and Territories (NCCT) identified by FATF as having significant deficiencies in their AML systems, or not having any systems at all. At present, there are 2 entries on the NCCT list: Myanmar (Burma) and Nigeria. Countries are added to or removed from the NCCT list based on their efforts in implementing legislation and adequate procedures to address money laundering and terrorist financing. Inclusion on this list can have significant impacts on the ability of the country's government, businesses and citizens to conduct cross-border financial transactions, especially with or involving U.S. financial institutions.

44/ This summary does not include a complete list of entities that have been designated as PMCLs but have yet to be subject of a final rule imposing a particular special measure against them (for example, Infobank from Belarus, First Merchant Bank from the Turkish Republic of Northern Cyprus and its subsidiaries, etc.)

45/ These activities would be highly unusual for a university credit union but, to the extent a credit union were to engage in such activities, additional BSA provisions would apply.

C. Reporting Requirements

As noted above, the U.S. Government has established a fairly complex reporting system through the BSA and the USA PATRIOT Act. Reporting obligations related to cash transactions (receipt or transportation cross-border) apply to all persons in the United States (including businesses and institutions). The obligations to file mandatory reports of suspicious activities applies only to certain financial institutions covered by the BSA for which FinCEN has issued final regulations that require such reporting (of course, financial institutions not yet covered by the mandatory suspicious activity reporting could file voluntary reports on suspicious activities). Finally, U.S. persons are individually responsible to report any interests in a foreign account. As a result, this overview addresses the following types of reporting obligations:

1. Suspicious Activity Reporting (SAR);
2. Reporting of cash transactions (CTR or FinCEN 8300 reports);
3. Reporting of transportation of currency across border (FinCEN 105); 46/
4. Reporting of interests in foreign accounts (Treasury Form TD F 90-22.1).

1. Suspicious Activity Reporting (SAR)

Under the BSA implementing regulations, credit unions are required to report suspicious transactions by filing Suspicious Activity Reports (SARs). SAR filing remains voluntary for financial institutions that are either exempt from this reporting (e.g., SVCs issuers) or are not yet subject to SAR requirements (e.g., "loan or finance companies").

Elements of mandatory SAR reporting:

- $5,000 threshold to trigger mandatory reporting (if a transaction is below $5,000, voluntary SAR may be filed)
- Suspicious transactions are not limited to those involving cash or cash equivalents (SAR reporting applies to wire transfers, checks etc.)
- File SARs within 30 days, in most cases;
- Document retention period is 5 years;
- After filing a SAR, the institution is prohibited from disclosing the filing to the customer (i.e., there is no "tipping" of customers regarding SAR filing)

A particular transaction would be considered "suspicious" if the credit union knows, suspects, or has reason to believe that the transaction:

- Involves funds derived from illegal activity or is intended to hide or disguise such funds;
- Is designed, through structuring or otherwise, to evade cash reporting requirements;
- Has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would be expected to engage (and the institution knows of no reasonable explanation for the transaction);
- Involves the use of the financial institution to facilitate criminal activity (e.g., the use of legally derived funds that are suspected of being used for a criminal purpose such as terrorist financing).

46/ FinCEN Form 105 was formerly Customs Form 4790.

Determinations with respect to mandatory SAR filing are made based on all the facts and circumstances relating to the transaction. In order to be in a position to determine whether a particular activity is suspicious, the institution has to know the customer's usual activities. The institution's SAR monitoring may, and should, be integrated within the establishment and implementation of an AML Compliance Program under section 352. Credit unions should not rely solely on their existing measures to combat fraud in lieu of having a formal Compliance Program – such measures may be useful for SAR purposes but not sufficient to satisfy the BSA requirements.

While the BSA and implementing regulations do not contain a particular list of "red flags" or high risk transactions specific to universities, credit unions generally should watch for transactions that do not make economic sense or are unusual for the particular customer (or customer type). Specifically, watch for transactions that are, or involve:

- unusual size, frequency or type
- inconsistent with normal customer activity
- beyond customer's financial means
- funds received by third party check
- unusual processing instructions
- unusual use of an intermediary

Also, credit unions may want to watch for:

- Customers from countries on the NCCT list (or sending payments from such countries);
- Customers from narcotic source countries (e.g., Colombia—there is both AML risk and OFAC risk because a number of SDNs are located in Colombia);
- Pattern of frequent overpayment (e.g., tuition overpayment every semester);
- Pattern of early loan repayment (e.g., taking out a loan, followed by full repayment and another loan within a short time frame);
- Customers acting on behalf of others, with no apparent connection;
- Customers unwilling to provide identifying information;
- Early withdrawal from enrollment and request for tuition refund; and
- Excessive amounts of transactions using SVCs.

2. Reporting of "Cash" Transactions (CTR or 8300 Reports)

All U.S. businesses and institutions have been subject to "cash" reporting requirements under section 6050I of the IRC and applicable Internal Revenue Service regulations, even before the enactment of the USA PATRIOT Act. 47/ The USA PATRIOT Act's section 365 and FinCEN's implementing regulations codified these reporting requirements within the BSA (FinCEN's regulations also clarified that only one report needs to be filed, separate reports under IRC and BSA are not required). 48/ Under the applicable regulations, any person who, in the course of a trade or business, receives "cash" in excess of $10,000 in one transaction (or two or more "related transactions") is required to report the receipt of cash by filing FinCEN Form 8300. Financial institutions covered by the BSA (such as credit unions) are subject to the same reporting requirements, albeit under a different

47/ *See* 26 C.F.R. § 1.6050I-1.
48/ *See* 31 C.F.R. § 103.30.

regulatory provision, and are required to report the receipt of cash by filing FinCEN Form 104, Currency Transaction Report (CTR). 49/

Accordingly, all universities and credit unions are required to report the receipt of "cash" that totals more than $10,000 in single transaction (or a series of related transactions). Tuition payments in installments would be considered a "series of related transactions" so if payments are made in "cash," the university would need to assess whether the reporting requirement is triggered.

For purposes of this reporting obligation, the term "cash" includes coin and currency as well as enumerated monetary instruments (i.e., a cashier's check, bank draft, traveler's check, and money order) having a face amount of $10,000 or less but only when such monetary instrument is received:

- In a "designated reporting transaction" (i.e., a retail sale of a consumer durable, a collectible, or a travel or entertainment activity), or
- In a any transaction in which the recipient knows that such monetary instrument is being used to avoid triggering the reporting requirement (i.e., the recipient knows that the instrument is being used to "structure" payments to avoid triggering the $10,000 threshold). 50/

Case Study: A foreign student opens an account at the university's credit union and deposits $9,000 in cash (currency). He returns for three days in a row and deposits $4,000 in money orders each day, grumbling that it would be "so much easier" if he were "allowed" to deposit all of his money at once. A week later, he receives a wire transfer of $45,000 from an off-shore trust account. He then takes out a loan in the amount of $50,000 and repays it within a month, with another funds transfer from a different off-shore account. He is now asking for a second loan of $50,000.

Q. Is this suspicious and what should the credit union do?

A. With respect to the student's initial deposits, the credit union likely would have to file a CTR (FinCEN Form 104) for the receipt of cash and "cash equivalents" in excess of $10,000 in a series of related transactions. Even though his money orders had a face value of less than $10,000, based on his comments and behavior, the credit reason may have reason to know that he's been "structuring" his money order deposits to avoid triggering the reporting threshold. As a result, the money orders would be deemed "cash" for purposes of CTR reporting and, when aggregated with his initial currency deposit, exceed $10,000 in a series of related transactions.

With respect to the loans and funds transfer activity (and in light of his initial deposit activity), the credit union also may have to file a mandatory SAR because the activities involve more than $5,000, are inconsistent with normal student account activity, and are unusual in frequency and type. The credit union would have 30 days from his last loan request to file a SAR. Finally, the credit union cannot tell the student that a SAR had

49/ *Id.* § 103.22.
50/ *Id.* § 103.30(c)(1); 26 C.F.R. § 1.6050I-1(c)(1).

been filed (no "tipping" allowed) and it would have to keep all the records related to these transactions for 5 years from the date of SAR filing.

3. Reporting of Cross-Border Transportation of "Cash" (FinCEN 105)

Under applicable Treasury regulations, a person in the United States who receives currency or "monetary instruments" in an aggregate amount exceeding $10,000, which have been transported, mailed or shipped to the United States from a third country, must report the receipt of such cash or monetary instruments. 51/ The report is filed by submitting FinCEN Form 105 (formerly Customs Form 4790). This reporting obligation does not apply if the person who transported or mailed the cash/monetary instruments that exceed the threshold amount had already declared the funds to U.S. authorities upon arrival to the United States and filed the same FinCEN Form 105. We also note that this reporting requirement would not be triggered by a transfer of funds through normal banking procedures that does not involve the physical transportation of currency or monetary instruments across the U.S. border.

For purposes of this reporting obligation, the term "monetary instruments" does not include checks that bear restrictive endorsements. For example, a check made payable to John Doe and endorsed on the back by Mr. Doe's signature and the words "For Deposit Only" would bear a restrictive endorsement and thus would not be considered a monetary instrument that could trigger this reporting requirement. If, however, the same check is merely endorsed (signed) on the back by Mr. Doe, such document represents a bearer instrument (it could be cashed by anyone in possession of the document) and would be deemed a monetary instrument that could trigger the reporting requirement.

Case Study: A U.S. student came to the Registrar's office to pay $15,678 in tuition, fees, room and board for the semester. He took $16,000 in $100 bills out of a duffel bag, with a lot of money still visible in the bag. The bag had a yellow Lufthansa name tag and a white luggage destination tag marked "JFK" still attached, looking like it just came from an airport. He also inquired whether the university offers safe deposit boxes that he could rent for the year. The Registrar's office employee took the money, scanned it for counterfeit currency, and processed his payment (the employee also told the student that the university does not offer safe deposit boxes but that it has a credit union where the student could open an account).

Q. Has the employee done anything wrong?

A. The employee was correct to process the transaction but the university will need to file an 8300 report for receipt of cash in excess of $10,000 and also may need to file a FinCEN 105 report for transportation of currency. Under these circumstances, the employee should have inquired whether the student brought the money into the United States and, if so, whether he reported it to U.S. authorities upon arrival. If the student brought the money in but did not report it, the university has just received more than $10,000 in cash that was physically transported into the United States. As a recipient of such funds, the university would have to report it by filing the FinCEN 105 form. In addition, in light of the unusual circumstances of this case, the university also would want to consider filing a voluntary SAR.

51/ *See* 31 C.F.R. § 103.23.

4. Reporting of Interests in Foreign Accounts (TD F 90-22.1)

Each U.S. person who has a financial interest in or signature authority (or other authority) over any financial account (e.g., bank account, securities account) in a foreign country must file an information report to the U.S. Government. 52/ No report is required if the aggregate value of the account(s) did not exceed $10,000 at any time during the calendar year. The report is submitted on Treasury form TD F 90-22.1 on or before June 30 of the succeeding year (i.e., if a person had $50,000 at a foreign bank account at any point during calendar 2005, the report would be due on June 30, 2006). This report is not filed with a person's U.S. income tax return and should not be mailed to the Internal Revenue Service along with the taxpayer's income tax return.

For purposes of this reporting, the term "U.S. person" means a citizen or resident of the United States, a domestic partnership, a domestic corporation, or a domestic estate or trust. Reporting obligation rests on the person with a financial interest in the account—for example, each student or staff member who has such financial interest in a foreign account must, on his or her own, comply with the reporting requirement. The university would not be responsible for students or staff members who fail to submit these reports.

* * * *

In light of the broad scope of OFAC sanctions regulations and AML provisions set forth in the BSA and the USA PATRIOT Act, universities need to understand these restrictions and take steps to comply with the applicable compliance and reporting obligations. Universities also should monitor developments in these areas to ensure ongoing compliance.

52/ *Id.* § 103.24.